REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
11-27-2007	FINAL	

4. TITLE AND SUBTITLE

Data Mining and Information Technology:

Its Impact on Intelligence Collection and Privacy Rights

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

LCDR Eric Soderberg

Paper Advisor (if Any): William Glenney, SSG Deputy Director

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Strategy and Policy Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPOR NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted as an independent research project in the Advanced Research Program, Center for Naval Warfare Studies, U.S. Naval War College. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

Modern Information Technology (IT) has radically magnified the capability and power of data mining. At a time when the threat environment has shifted in emphasis to COIN, terrorism, and cyber war, IT-enhanced data mining capabilities could provide some of the critical intelligence demanded by these types of threats. Yet depending on how this new capability is employed and what protections are in place, US citizen's privacy rights could be threatened.

This paper establishes the intersection between the capability and need for data mining and the suitability of existing policy to enable its legitimate application. Policy recommendations are made to address the concerns discussed above and facilitate the fullest execution of the National Strategy for Information Sharing.

15. SUBJECT TERMS

Data Mining, Privacy, Information Technology (IT), Cyber war, National Information Strategy

16. SECURITY CLASSIFICATION OF:	17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PER
			Chairman, S+P Dept

a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER *(include area code)*
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED		32	401-619-1894

Standard Form 298 (Rev. 8-98)

U. S. Naval War College
Newport, Rhode Island

Data Mining and Information Technology:
Its Impact on Intelligence Collection and Privacy Rights

by

Eric Soderberg
Lieutenant Commander, United States Navy

This paper was completed as an independent research project in the Advanced Research Program, Center for Naval Warfare Studies, U.S. Naval War College. It is submitted to the faculty of the Naval War College in partial fulfillment of the academic requirements for the degree of Master of Arts in National Security and Strategic Studies. As an academic study completed under faculty guidance, the contents of this paper reflect the author's own views and conclusions, based on independent research and analysis. They do not necessarily reflect current official policy of any department or agency of the U.S. government.

Advanced Research Project
Fall Term, Academic Year 2007-2008
26 November 2007

Abstract

Modern Information Technology (IT) has radically magnified the capability and power of data mining. At a time when the threat environment has shifted in emphasis to COIN, terrorism, and cyber war, IT-enhanced data mining capabilities could provide some of the critical intelligence demanded by these types of threats. Yet depending on how this new capability is employed and what protections are in place, US citizen's privacy rights could be threatened. Overly intrusive data mining efforts by the US government may not only threaten citizen's privacy rights but generate political and social resistance to data mining which could undermine its effective use for security and law enforcement purposes. Additionally, commercial enterprises, foreign governments, criminals and terrorists also use IT enhanced data mining to efficiently gather a wide spectrum of intelligence, leaving many Americans vulnerable to a range of consequences.

This paper establishes the intersection between the capability and need for data mining and the suitability of existing policy to enable its legitimate application. Specific problems identified and focused on are: 1) The government does not always have legal access to data needed to meet some of its most pressing security intelligence demands. 2) Data related to US citizens collected by commercial activities is unnecessarily vulnerable to exploitation and abuse. 3) The current legal framework governing access to commercial data bases leads to a false dichotomy between providing intelligence and protecting privacy in that the capability to tailor and control data base access allows valuable intelligence to be gathered while still protecting private data. Policy recommendations are made to address the concerns discussed above and facilitate the fullest execution of the National Strategy for Information Sharing.

Table of Contents

Introduction

Modern Information Technology (IT) has radically magnified the capability and power of data mining. It has the potential to provide critical capability to US military, intelligence and law enforcement agencies. Yet depending on how this new capability is employed and what protections are in place, US citizen's privacy rights could be threatened. Overly intrusive data mining efforts by the US government may not only threaten citizen's privacy rights but generate political and social resistance to data mining which could undermine its effective use for security and law enforcement purposes. In addition to concerns over US governmental intrusion and privacy invasion, commercial enterprises, foreign governments, criminals and terrorists also use IT enhanced data mining to efficiently gather a wide spectrum of intelligence, leaving many Americans vulnerable to a range of consequences.

Resolving how data mining will be employed and how sensitive or private information will be protected is an important element in executing the National Strategy for Information Sharing. The National Strategy for Information Sharing is focused on improving the sharing of homeland security, terrorism, and law enforcement information within and among all levels of governments and the private sector. The strategy also recognizes that "it will remain essential to continue to protect the information privacy and other legal rights of Americans as we protect our Nation. Accordingly, our efforts will remain relentless on two fronts -- protecting our people, communities, and infrastructure

from attack and zealously protecting the information privacy and other legal rights of Americans." [1]

This paper describes the process of data mining in greater detail, with an emphasis on how modern IT has dramatically increased data mining's utility, creating essentially a new capability available to a wide variety of actors. The current threat environment facing the US is evaluated and contrasted with historical norms to demonstrate the need for the types of information that IT enabled data mining can help obtain. With the intersection between the capability and need for data mining established, the suitability of the existing legal and policy framework to enable its legitimate application is discussed. Specific problems identified and focused on are: 1) The government does not always have legal access to data needed to meet some of its most pressing security intelligence demands. 2) Data collected by commercial activities in the course of their normal business operation is unnecessarily vulnerable to exploitation and abuse. 3) The current legal framework governing access to commercial data bases leads to a false dichotomy between providing intelligence and protecting privacy in that the capability to tailor and control data base access allows valuable intelligence to be gathered while still protecting private data.

Finally, this paper will provide conclusions and policy recommendations to balance intelligence collection with privacy concerns and facilitate the fullest execution of the US strategy for information sharing.

Notes

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography.)

1. US President, *National Strategy for Information Sharing*, 1.

Data Mining

Data mining is a process in which raw data is collected and analyzed to produce information or knowledge.[2, 3] Data mining has the following major elements: collecting data, classifying and storing it in a structured format, analyzing it for relationships, and presenting the data in a useful format. The particular relationships sought vary among the available data, individual applications and goals. The structure and relationships discovered among the raw data can provide as much value and knowledge as the data itself.[4] Information Technology, including the Internet, brings two principle changes to data collection and mining: 1) The volume and variety of data available have increased exponentially, and 2) The cost in terms of time and money required to classify, analyze for relationships, and extract useful knowledge has decreased exponentially.

2. Peter Cabena, Pablo Hadjnian, Rolf Stadler, Jaap Verhees, Allesandro Zanasi, *Discovering Data Mining: From Concept to Implementation.*

3. The military has long acknowledged the power behind data mining and analysis. Operation Security (OpSec) is the terminology used for the effort to deny the enemy the capability to determine operationally important information via the collection, mining and analysis of unclassified data. It is different from the effort to secure classified information. Classified data, even in isolation, has been determined to have value to potential adversaries, and is tightly controlled with well established procedures to avoid release. OpSec deals with everything else, data which in isolation may not provide valuable information, but when subject to data mining and analysis, could yield usable information to an enemy.

4. This relational information about a data set is sometimes referred to as metadata.

Information Technology and Data Collection

The sensors and data sources available via modern IT vastly expand the ability to collect data. Improvements in their capability are running in rough balance with improvements in electronic processor capability, which continues growing in accordance with Moore's law, doubling approximately every 18 months. Examples of common sensors and potential data sources include:

Cameras - Digital cameras (still and video) have been improving in capability while simultaneously dropping in cost at a rate commensurate with the rest of IT. Cameras can be found on: satellites in orbit, Unmanned Aerial Vehicles (UAVs), poles monitoring traffic intersections, Automatic Teller Machines (ATM's), police cruisers, and web cams. Small cameras are carried by people as stand alone devices or embedded in cell phones. Digital cameras can be found almost anywhere. In some cities, such as London and New York, the extent of camera deployment is such that it is almost impossible to avoid being seen. In Britain, which has the same 10 to 1 person to camera ratio as the US, it is estimated that the average citizen is caught on camera 300 times each day.[5] The power of extensive video coverage is magnified greatly by the nascent capability for voice and facial recognition technology to identify specific individuals on camera.

Navigation Systems - Global Positioning Satellites (GPS), inertial navigation, and radio triangulation provide the technical means to accurately determine a geographic position on the earth. Under Federal Communication Commission (FCC) regulations,

5. Unattributed, *Learning to live with Big Brother,* Economist Magazine.

new cell phones are required to have the capability to automatically report their location when making 911 calls.[6] Not only will position (of a device and its user) be determined, but with the proliferation of mobile connectivity, it is very likely this information will be shared and subject to collection. This sharing will be done for a variety of purposes such as to facilitate the gathering of data tailored to that particular location (such as local goods and services available), to call for aid in case of emergency (OnStar or 911), or simply to meet friends.

Communication logs - Traditional phone logs have long been useful sources of information, providing evidence of a user's location and contacts. The portability of cell phones adds to this capability because the typical cell phone travels with, and is more easily tied to, a single individual. Internet Service Providers (ISP) data logs track all online activity - every site visited, on-line newspapers read, and people Emailed. As cyberspace becomes ever more integrated into our social and economic way of life, the quality and volume of data available for collection via ISPs will continue to grow.

Biometrics - Another critical and growing capability for collecting personally identifiable data is referred to as biometrics. Using a variety of technical means, some requiring voluntary participation and proximity but others not, finger prints, retinal or iris scans, facial recognition, voice recognition, and DNA can be used to positively identify a person. The 4.6 million DNA profiles in US federal data banks are an example of how widespread the use of these biometric identifiers has become.[7]

---

6. Enhanced 911 (E911) allows emergency dispatchers to pinpoint the location of someone who calls 911. The primary objective, the FCC says, is to ensure rapid emergency response and save lives.

7. Unattributed, *Learning to live with Big Brother,* Economist Magazine - These DNA profiles are primarily from convicted felons.

Self Dissemination/electronic tags - Information that can be collected on an individual is significantly augmented by data that they themselves provide; participating in any number of transactions such as staying at a hotel, getting a job, paying taxes or getting a loan requires significant releases of information such as name, birth date, social security number, income statements, address, and type/make of vehicles with license plate numbers. Individuals expedite transactions by carrying positive identification such as credit or debit cards, where purchases are recorded along with date, time and location. RFID tags, such as EZpass, allow the collection of this type of data to happen even more quickly and at a distance. People also voluntarily link information to the Internet, about themselves or others, via a multitude of venues such as blogs, message boards, My Space profiles, or Second Life Avatars.

News Outlets/Educational Institutions/Retailers - Almost every traditional source of information is now mirrored with a presence on the Internet. News outlets from every medium, universities, retailers, and many bureaucracies have digitized their information and made it available via the Internet, where it is easily accessed and amenable to data mining.

The range and variety of data collection methods and devices make the quantitative increase in the ability to economically collect data so substantial that it arguably represents a new capability. In the past, much of this same information could have been collected against a particular target, but it would have entailed significant and possibly unacceptable cost and man power. IT enabled collection has significantly reduced the cost and made the *incremental* cost of an additional target negligible.

Information Technology and Data Mining

The connectivity of cyberspace, along with faster processors and advanced algorithms, allow routine mining and analysis of massive volumes of data from all over the globe. Data mining tasks that in the past would have been only theoretically possible to complete because of time and cost constraints are quickly and cheaply accomplished. Just as with data collection, advances in IT have increased the scale and dropped the cost of mining data to such an extent that, although the basic process is old, the capabilities are essentially new.

With unfettered access to data gathered by government, commercial activities, and individuals, the technological capability exists to build detailed biographies and profiles, current up to near real time, with negligible incremental cost per target. Along with individual pieces of information such as a person's location, financial status, purchases, personal contacts, and political affiliation, a deeper understanding of an individual's behavior can be discerned and modeled. Armed with this model, behavior can be predicted and manipulated.[8] In an environment where these capabilities are common place, the value of data becomes increasingly contextual. Depending on how a particular piece of data is combined with other data sets, for what purpose, and with whom it is shared, the data or resulting information could be trivial or incredibly sensitive and private.

8. From Microsoft data mining software sales information: "You use a Prediction model to provide real-time purchase recommendations to users visiting your site, and to guess unknown profile properties about users. For example, a Prediction model may say that if a visitor to your site is male, over 55, and purchases sports clothes, then he is also likely to purchase golf equipment. You can use this model to make real-time recommendations for golf equipment to users who match this profile. Prediction models typically provide recommendations that are more accurate than human-generated rules, as they predict based upon the previous activity on the site." http://msdn2.microsoft.com/en-us/library/, (accessed online 10/10/07).

Changing Threat Environment and Intelligence Requirements

The probability of high intensity conflict and the degree to which the nation should prepare for it is a hotly debated topic.[9] However, with the fall of the Soviet Union, the ongoing conflicts in Iraq and Afghanistan, and the worldwide effort against Al Qaeda, it is clear that the relative probability of occurrence of traditional force-on-force, high intensity conflict has declined in relation to insurgencies, irregular warfare, terrorism, organized crime and cyber warfare.[10] This shift and increased emphasis are highlighted in The National Strategy for Information Sharing, The National Strategy for Combating Terrorism, The National Strategy for Homeland Security, and The National Intelligence Strategy. Some of the specific requirements and considerations for Counter Insurgency (COIN), Anti-Terrorism and Cyber warfare are expanded upon below to demonstrate how US intelligence requirements have shifted in response.

9. Thom Shanker, *Joint Chiefs Chairman Looks Beyond Current Wars,* New York Times, 8: "Admiral Mullen expressed worries that the missions in Iraq and Afghanistan had undermined the military's ability to fight big wars — and distracted the armed forces from preparing to face other threats. "Current combat efforts are so heavily focused on counterinsurgency missions that the Army and Marine Corps "haven't been training in or focusing on this wider spectrum of requirements should we need to be called to do something else," Admiral Mullen said. "And so we've got to make sure that we can train to, equip to and be ready for just a broader spectrum of missions."

10. Secretary of Defense William Gates speaking to a gathering of current and retired soldiers about the wars in Iraq and Afghanistan, which he said would "remain the mainstay of the contemporary battlefield for some time" and "Success will be less a matter of imposing one's will and more a function of shaping behavior of friends, adversaries, and most importantly, the people in between." Future conflicts, he said, "will be fundamentally political in nature and require the application of all elements of national power" with an implicit warning for the Army not to retreat in its manning, equipping and training to the more familiar task of conventional, high intensity combat.

COIN intelligence considerations: While one might conclude that a military equipped and trained for high intensity combat operations could conduct COIN as a lesser included mission set, this has been repudiated by experience in both Vietnam and Operation Iraqi Freedom (OIF).[11] While COIN requirements may overlap to some degree with those for high intensity combat operations, it has some unique demands, which extend to the intelligence domain. The collection of intelligence from identified adversaries, as is the basis for an intelligence apparatus built with high intensity combat operations as the principal threat, is not sufficient for COIN.[12,13] The Army Field Manual on Counterinsurgency discusses COIN intelligence: "Counterinsurgency (COIN) is an intelligence-driven endeavor and… intelligence in COIN is about people. US forces must understand the people of the host nation, the insurgents, and the host-nation (HN) government. Commanders and planners require insight into cultures, perceptions, values, beliefs, interests and decision-making processes of individuals and groups. These requirements are the basis for collection and analytical efforts."[14]

The local nature of insurgencies, the rapidity with which they evolve, and the myriad of cultural and human factors make analysis of the intelligence extremely

---

11. "The idea that if you just train high-intensity conflict then you can go to Iraq and do counterinsurgency - everybody realizes that was wrong." Brig. Gen. Ed Cardon, the 3rd ID's assistant division commander. From Greg Grant, *Back to Iraq,* Government Executive, April 1, 2007, Posted online at www_GovernmentExecutive_com.htm.

12. "Today's intelligence paradigm, which emphasizes the acquisition of secret intelligence from foreign governments, may be ill-suited to modern counterinsurgency. Secret intelligence is often less relevant than information which is not classified by any government, but is located in denied areas. Human intelligence and tactical signals intelligence are clearly crucial, and additional effort in these areas would be valuable." From David Kilcullen, *Counterinsurgency Redux,* 8.

13. "Intelligence personnel should think differently and be proactive in their collection, analysis, and planning by breaking from the traditional warfare mindset when engaged in irregular warfare." From the Air Force Doctrine Document 2-3*, Irregular Warfare*, 45.

14. Department of the Army, FM 3-24, *Counterinsurgency.*

complex. In many ways, intelligence analysis in counterinsurgency has more in common with law enforcement than conventional, high intensity combat.[15]

Anti-terrorism intelligence considerations: In part because terrorism is often used by insurgents, anti-terrorism intelligence requirements are very similar to those of COIN. However there are two important additional complicating factors for US anti-terror efforts. First, unlike COIN, there is the far greater likelihood that some of the targets will be US citizens or residents. Secondly, the indefinite nature of the "Long War"[16] against terrorism demands that whatever action is taken, it must be acceptable to the US populace over an extended period of time. These factors bring operations closer to law enforcement, and introduce additional layers of legal and political complications to surveillance and the collection of data to support anti-terrorism actions.

Cyber warfare intelligence considerations: While there is a physical component to cyber warfare, more than in any other domain, the intelligence aspect dominates. Surveillance is a prerequisite for both offensive and defensive operations. For offensive purposes, determining details about an adversaries network, such as Operating System (OS) in use, ports open, firewalls active, applications employed, and hardware being used, is a virtual prerequisites for an attack. Additionally, there is an offensive cyber warfare element directly related to human intelligence (HUMINT). This element is

15. Sweet, Jonathan E.; Teamey, Kyle, *Organizing Intelligence for Counterinsurgency.*

16. "The War on Terror will be a long war." US President, *The National Strategy for Combating Terrorism.* That the term "The Long War" is often used synonymously with the Global War on Terror, in official policy and elsewhere, is a good indication of the anticipated duration of the effort.

referred to as "social engineering", and it involves exploiting people with legitimate access to a computer system or network and manipulating them to take action or provide information which then allows the hacker to gain access.[17]

For defensive purposes, two principle tactics are: 1) determining a baseline of legitimate and "normal" activity for data transfers in order to detect anomalies[18,19] and 2) the detecting, cataloging, and distributing of known attack modes and vulnerabilities to produce counter measures.[20] It is often difficult if not impossible to have a priori knowledge of the identity of potential attackers, as their activity is mixed into the massive background noise of legitimate data traffic. Even in those instances where a compromise has been detected, attribution for the attack often remains a significant challenge. Cyber warfare intersects with law enforcement because it is not always possible to immediately distinguish whether an attack originated from a state actor, terrorist or criminal, and because most attacks are in fact criminal in nature.[21]

---

17. Kevin Mitnick, William Simon, Steve Wozniak, *The Art of Deception.* Kevin Mitnick was a somewhat notorious hacker arrested in the 1990's. Social engineering was among his favored tactics.

18. This is often accomplished by conducting data mining. A principle example is the System for Internet-Level Knowledge. As described on by CERT, it is a collection of traffic analysis tools developed by the CERT Network Situational Awareness Team to facilitate security analysis of large networks. The SiLK tool suite supports the efficient collection, storage and analysis of network flow data, enabling network security analysts to rapidly query large historical traffic data sets.

19. Michael Collins, Timothy J. Shimeall, Sidney Faber, Jeff Janies, Rhiannon Weaver, Markus De Shon, *Predicting future botnet addresses with uncleanliness.*

20. Bruce Schneier, Lance Spitzner, *Know Your Enemy*. This book lays the foundation for the Honeynet Project. The Honeynet project is a volunteer organization that intentionally links computers and networks with known vulnerabilities to the internet with the aim of soliciting attacks. By monitoring these systems as they are attacked and compromised it is possible to determine the methodology of various attacks and discover flaws in defenses which could lead to other systems being compromised. This information is then widely distributed to aid the creation of "patches", update anti-virus and firewall software, or other fixes that minimize vulnerabilities.

21. "Malicious attacks are increasingly being carried out for very specific reasons. Cyber criminals are using bot-nets, denial-of-service extortion attacks, and sophisticated identity theft techniques for financial gain." Howard G., *The True Nature of Cyber Crime,* 16.

Five key points and commonalities that must be considered in meeting the information needs of organizations involved in the COIN, anti-terrorism and cyber warfare mission sets discussed above are:

1. Identifying adversaries who often intentionally hide amongst neutral or friendly populations is emphasized rather than the more traditional intelligence requirement of collecting on a known, clearly identifiable adversary.
2. Preventing adversary action in addition to responding to it is a primary goal.
3. They are interagency missions; intelligence will often be collected and used by multiple agencies. Raw data will often come from commercial and open sources.
4. There is not always a clear separation between combat and law enforcement.
5. The relative importance of these missions has increased versus conventional high intensity combat.

Because much of the US Cold War intelligence gathering equipment and capability was directed towards high intensity combat operations, the ability to collect the types of intelligence discussed above is not as robust as it otherwise might be. Additionally, many of the traditional means to meet these requirements rely on HUMINT, which is not a capability that can be fielded or upgraded without significant lead time and resources.[22] Even with the time and resources, meeting these requirements is very difficult relying on traditional intelligence collection methods alone. These factors highlight the importance of data mining because it is a tool set well suited to help

---

22. Lieutenant General Thomas F. Metz, Colonel William J. Tait, Jr., and Major J. Michael McNealy, *OIF II, Intelligence Leads Successful Counterinsurgency Operations.*

fill these particular voids, and do so relatively economically. However, data mining by the US government in order to meet the intelligence requirements discussed above, or by others, could also impact US citizen's privacy rights.

Privacy Rights

The right to privacy is not explicitly delineated in the US constitution. However, via judicial precedent and policy it flows from the First[23] and Fourth Amendments.[24,25] As described by that precedent and policy, privacy rights are inherently entwined with public "expectations" of what is in fact private versus public. So while the right to privacy is well established legally, the specifics are fluid, changing as public opinion evolves and precedents are set.

Many of the constitutional and policy privacy protections the US currently employs are targeted at the government and are focused on how data may be collected.[26] Restrictions on data collection rest on a few central concepts. First is the distinction between what is public and what is private: Public data can be collected and activity in

---

23. Amendment I to the US Constitution:
Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.

24. Appeal from the Supreme Court of Errors of Connecticut, ^ ***Griswold v. Connecticut***.

25. Amendment IV to the US Constitution:
The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

26. United States Congress, *The Privacy Act of 1974.*

public can be observed, that which is private cannot. There may be a wide variety of views on what should be private or public, but US law, policy and judicial precedents roughly conform to the following summary: Private information is that personal information disclosed in a private place with the expectation that it will remain confidential and not be disclosed to third parties. A private place is one where there is a reasonable belief that a conversation or activity can not be heard or observed by others acting in a lawful manner (such as a home or hotel room).[27] Thus in practice, the protection for any individual piece of data is often predicated more on the manner and circumstances in which it may be collected than on any assessment of its intrinsic sensitivity. Even after data is lawfully collected, the government is restricted in how it can be used or disclosed by law.[28] With a few exceptions, commercial enterprises can create their own individual privacy policies that dictate what they will do with lawfully collected data.

A second concept for protecting privacy is judicial oversight of the executive branch. In general, the government does not have the right to unilaterally acquire private data on its citizens without their consent. When there is pressing law enforcement or security need to collect private data, given probable cause, a judge can issue a warrant. The warrant is not a "free pass" to ignore privacy rights; it targets particular individuals and locations, and is valid for limited periods of time and only for specified purposes.

27. Christopher Slobogin. "Technologically – Assisted Physical Surveillance: The American Bar Association's Tentative Draft Standards" Harvard *Journal of Law & Technology.* Volume 10, Number 3.

28. United States Congress, *The Privacy Act of 1974.*

Another concept for protection is afforded by the divisions drawn by US law between foreign intelligence collection and domestic law enforcement through acts such as the Electronic Communications Act (ECA)[29], the Foreign Intelligence Surveillance Act (FISA)[30], Titles 10 and 50 of the US Code, and the Posse Comitatus Act. US government agencies are individually tasked and authorized to collect intelligence on foreigners for security purposes or on citizens and foreigners for law enforcement, but generally not both. Recently some of these distinctions have been blurred in an effort to increase data sharing and cooperation between government agencies, particularly in standing up the Department of Homeland Security (DHS) and in the Patriot and Protect America Acts.[31] However there are still significant legal barriers to mixing roles and responsibilities for foreign intelligence gathering and domestic law enforcement.

29. United States Congress, *Electronic Communications Privacy Act of 1986*.

30. United States Congress, *The Foreign Intelligence Surveillance Act of 1978*.

31. United States Congress, *Protect America Act of 2007*.

Data Access for Intelligence Data Mining

The US government is in fact conducting wide spread data mining; as of 2005, there have been over 200 government data mining programs from agencies such as the DoD, DHS and FBI and there has been significant concern among US citizens and Congress with this action because the value of these programs and their cost to privacy as carried out under current law is uncertain.[32,33]

The authority the government exercises to access data collected by commercial enterprises is largely predicated on its ability to generate probable cause prior to accessing said data. The government has argued that when the greatest intelligence need is to identify suspects in the first place, and to preempt adversaries prior to attack, this scheme significantly limits the potential value of data mining for US security.[34] Without modification to our current laws, effective use of data mining for security purposes will be curtailed at significant opportunity cost.[35] This pressing need is demonstrated by policy and legislative attempts to arrange for wider access.[36,37] However, proposals to

32. Economist Magazine, *Learning to live with Big Brother.*

33. Examples of some of the better known data mining programs: Carnivore, Total Information Awareness (TIA), Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement (ADVISE), and the Multistate Anti-Terrorism Information Exchange (Matrix).

34. White House Fact Sheet from 8/5/07 referencing the Protect America Act - "Our work is not done… When Congress returns in September, the Intelligence Committees and leaders in both parties will need to complete work on the comprehensive reforms requested by Director of National Intelligence Mike McConnell."

35. Scott Shane and Eric Lichtblau, "Cheney Pushed US to Widen Eavesdropping", 1A.

36. US Congress, *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* (Public Law 107-56), also known as The Patriot Act, Library of Congress

37. US Congress, *Protect America Act of 2007.*

modify those laws to gain the desired level of access face significant constitutional[38, 39] and political resistance.[40]

There is also the risk that security concerns within our intelligence agencies become so great that data is collected outside our current legal constraints and without a pre-planned system for minimizing the impact to privacy rights.[41,42,43,44] The Watergate scandal provides historical precedent for this type of abuse. In its wake governmental intelligence gathering on US citizens was exposed in the Church Report,[45] and contributed to the subsequent increased oversight of the executive branch and the passing of the Foreign Intelligence Surveillance Act (FISA) of 1978. Some of the distinctions between foreign intelligence collection and domestic law enforcement made by FISA and ECA have become increasingly difficult to maintain given security requirements in the current threat environment. This is due to the difficulty of identifying adversaries who

---

38. Unattributed, *Federal judge rules 2 Patriot Act provisions unconstitutional,* CNN.com, September 26, 2007, accessed online at http://www.cnn.com/2007/US/law/09/26/patriot.act/.

39. Dan Eggen, "Key Part of Patriot Act Ruled Unconstitutional", A16.

40. Patrick Leahy, Senate Judiciary Committee, *Hearing on "Privacy in the Digital Age: Discussion of Issues Surrounding the Internet*". - " According to the Center for Social and Legal Research, 88 percent of Americans reported being "very" or "somewhat concerned" about threats to their personal privacy. I am pleased the Senate Judiciary Committee is taking this concern seriously, and beginning an examination of new Internet-related privacy issues."

41. Martha Mendoza, "US Police Surveillance Questioned" *Associated Press*, Posted Online at http://www.cbsnews.com/, April 6, 2003.

42. Scott Shane and David Johnston, "Mining of Data Prompted Fight Over US Spying", *New York Times*, July 29, 2007.

43. Jennifer Granick, "Nation's Soul Is at Stake in NSA Surveillance Case", online posting at http://www.wired.com/, (accessed August 15, 2007).

44. Michael Sniffen, "DHS Ends Criticized Data-Mining Program", Washington *Post/Associated Press*, Sep 5, 2007.

45. US Senate Select Committee to Study Governmental Operations, *Intelligence Activities and the Rights of American,* (The Church Report).

often mix freely within the general US population or with other friendly or neutral populations. Thus, some of the privacy protections specific to domestic use and US citizens increasingly conflict with security requirements.

Data Collected by US Commercial Activities Vulnerable

The free market recognizes that data bases, many with personal information, collected and mined with modern IT, have real economic value. This value is reflected in the multi-billion dollar market capitalization of corporations that have been built by turning that data into usable knowledge.[46] The outcome of this profitability is that commercial enterprises collect much of the data available on US citizens. This data has little protection; it can be sold or traded to almost anyone. Even information which is acknowledged in law as protected, such as personal medical records,[47] could likely be obtained by mining public, unprotected data. For example, given access to unprotected data such as clothes purchased, books ordered, web sites visited, and obituary notices, a variety of conclusions might be drawn. The size of pants ordered may indicate an overweight individual (diabetic risk factor), purchased books may have oversized font (indicative of poor eyesight, a symptom of diabetes), and internet logs might reveal multiple visits to sites such as WebMD and sites selling blood-sugar level testing equipment (aides in treating diabetes), and finally a review of obituary notices may reveal

46. Market capitalizations of information centric corporations: Google – $200 billion, AT+T - $250 billion, Ebay - $50 billion, Yahoo - $39 billion, Amazon.com – $37 billion, Priceline.com - $3 billion. Data from Yahoo finance 10/2007.

47. United States Congress, *Health Insurance Portability and Accountability Act of 1996(HIPAA),* Public Law 104-191.

a family member who died of diabetes (family history is a risk factor). The diagnosis and treatments prescribed for this condition, as handled by medical institutions and personnel, are controlled and protected. But by mining multiple unprotected sources of data, patterns of symptoms and risk factors may appear that would allow the protected information(diagnosis of diabetes) to be determined.[48]

As demonstrated above, data mining in particular has the capability to use unprotected data to reveal what is nominally protected information. Current US privacy protections are inadequate to control the collection and distribution of public data that can be mined to discover private information. While free market forces provide some control on the collection and use of personal data by commercial activities, the inability of citizens to readily assess the true value of the data they are revealing, the variety and complexity of corporate privacy policies, and a frequent lack of real alternatives to providing data, leaves this an incomplete mechanism for protecting privacy rights. The US is one of the few nations that rely so heavily on free market forces to protect privacy, ranking below 36 of 42 nations rated on the level of protections afforded its citizens.[49]

The massive amounts of available data can be a valuable source of intelligence for adversaries. Al Qaeda training manuals claim that more than 80% of its operational intelligence it gathers is from open or commercially available sources.[50] Plentiful data and advanced data mining potentially opens citizens to bribery, ID theft, harm or threats

48. Diabetic risk factors and symptoms from WebMD. Accessed online at http://www.webmd.com/.

49. US ranked below 36 of 42 nations rated by Privacy International on the level of protections afforded citizens. Privacy International (PI) is a human rights group formed in 1990 as a watchdog on surveillance and privacy invasions by governments and corporations.

50. Major Jason Densley, Lieutenant Julie Jansen, *The Impact of Social Networking on the Vulnerability of US Air Force Personnel to Adversary Influence Operations*.

of harm, blackmail, humiliation, propaganda, and kidnapping. Individuals in the military or security agencies may be even more susceptible to these consequences than the typical citizen due to their potential access to classified or sensitive information, their status as representatives of the U.S, and their relatively high rate of living and working overseas.

Conclusions and General Recommendations

Modern IT has radically magnified the capability and power of data mining. These new capabilities represent an opportunity to meet significant security needs of the US. At a time when threats to national security have shifted in emphasis to COIN, terrorism, and cyber war, IT enhanced data mining capabilities could provide some of the critical intelligence demanded. This is particularly important because other intelligence collection methods are either under resourced or incapable of meeting the new requirements. However, IT enhanced data mining by the US government or others pose a potential threat to US citizen's privacy. This threat is exacerbated when there is a lack of clear distinctions between national security and law enforcement mission sets, as is often the case in COIN, terrorism, and cyber war. This can make it increasingly difficult to maintain domestic privacy protections built on distinctions between foreign intelligence collection for national security and domestic law enforcement. The demand for knowledge, and data mining's capability to help provide it, will continue indefinitely, so resolving the tension between data mining and privacy rights will have long term consequences and is a necessary element to full execution of the US National Strategy for Intelligence Sharing.

Part of the solution is to break the false dichotomy between providing intelligence and protecting privacy. The two sets of requirements (intelligence collection and privacy rights), are at an impasse under the existing legal and policy framework in part because access to data has traditionally been a yes or no proposition. This fails to take full advantage of the flexibility IT provides to change not only the speed, but the manner in which tasks, such as searching a data base, are completed. Properly controlled and tailored access could minimize the exposure of private information while still supporting security and law enforcement operations. It need not be a zero sum trade-off between data mining and protecting civil liberties. An example of this type of tailored access is provided as a specific recommendation.

Additionally, US privacy protections continue to rely in large measure on distinctions in how data is collected. These distinctions are often irrelevant in light of the ability to produce information that citizens may expect to be private and protected by mining public, unprotected data. This leaves citizens unnecessarily vulnerable to having sensitive or private information exposed, with a variety of potential negative consequences for individuals, their employers, and society.[51] With an over-reliance on free market forces, data held by US commercial or private institutions is vulnerable to exploitation by data mining when compared to other nations. In the face of IT enabled data mining, US privacy protections are insufficient. US law and policy should acknowledge that some control and restriction on the use, retention, sale or distribution of personally identifiable data by commercial or private entities, beyond how it is collected, is necessary to preserve a meaningful degree of privacy.

51 Ibid.

Specific Recommendations

The impasse between US governmental access to commercially gathered data and privacy rights could be addressed by modifying the way in which warrants are issued and executed for searching data bases. Rather than attempt to force authorities to develop suspects and probable cause prior to gaining *any* access to commercially or privately held data, a data mining algorithm would be allowed to search across multiple data bases with the caveat that these searches would be limited - they would only be allowed to return names and other data when they indicate a pattern of behavior, which in its self would constitute probable cause. These searches would be approved and executed under court supervision.

For example, assume authorities are investigating a potential attack on a military base in the US. It might be determined by a judge that the purchase of large amounts of propane, the renting or purchasing of a van, and having been recently physically located near the base represents a pattern that justifies probable cause. The investigating agency would be allowed to have an algorithm search van rental records, propane purchases, and establish physical proximity by running facial recognition software on security videos and tracking cell phone usage in the local area. However, it would only return the names and data of those who correlated across all three criteria. Proceeding with a warrant obtained with such a justification would not allow unfettered government access to the data for everyone who purchased propane, rented a van or was captured on a video camera or made a phone call in the area. Thus, although a data mining algorithm might have access to a data base with sensitive or private information prior to establishing

probable cause, the investigating agency and individuals would not, keeping the procedure within the bounds of the Fourth Amendment.[52] Additionally, the results of such searches would also be treated as private information and have restrictions on its use and retention. In this manner the bulk of information on any given data base would remain protected, yet allow for authorities to greatly narrow their search for suspects. This proposal is in some ways an extension of the "minimize" procedures delineated in The Foreign Intelligence Surveillance Act.[53] In this case, protected data would be searched by an algorithm, but the privacy impact would be negligible because only data sets that met conditions of the court issued warrant would be returned as results.

A potential difficulty with this proposal is that the public may perceive the searching of protected data by the government, even if only by an algorithm and with effective "minimize" procedures, to be overly intrusive. However, the success of commercial services such as Gmail,[54] which scans the email traffic of its users with an algorithm to provide targeted advertising, suggests that most American's will accept this type of non-human intrusion given its benefits, even when the data being scanned has potentially private information. Another consideration is the difficulty in developing search algorithms that meet the probable cause standard; from a purely security minded outlook, simply having access to all the data and then finding a pattern would be easier. However, a degree of difficulty should not be a disqualifying factor if most of the desired

52. Amendment IV to the US Constitution:
The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

53. United States Congress, *The Foreign Intelligence Surveillance Act of 1978.*

54. It is estimated that there are 50 million Gmail users.

intelligence can, in the end, be attained and the alternatives for doing so are unworkable, unconstitutional or otherwise unacceptable to the US population.

A second specific recommendation is that the US should have federal privacy and data control laws that are more comprehensive than current statutes. The result should be that citizen's data have real and uniform protections regardless of which corporation or agency they are dealing with. An acceptable minimum baseline of protection would be implicit in all transactions. The basic protections recommended would follow the principles and standards described below:[55]

> **Notice:** Organizations must notify individuals about the purposes for which they collect and use information about them. They must provide information about how individuals can contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information and the choices and means the organization offers for limiting its use and disclosure.
>
> **Choice:** Organizations must give individuals the opportunity to choose (opt out) whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by the individual. For sensitive information, affirmative or explicit (opt in) choice must be given if the information is to be disclosed to a third party or used for a purpose other than its original purpose or the purpose authorized subsequently by the individual.

55. These principles are from the US Department of Commerce summary of requirements for compliance with "Safe Harbor" rules. "Safe Harbor" rules are designed to ensure that US corporations conducting transactions that require data transfers within or from E.U. nations meet minimum E.U. standards for privacy and data protection.

Onward Transfer (Transfers to Third Parties): To disclose information to a third party, organizations must apply the notice and choice principles. Where an organization wishes to transfer information to a third party that is acting as an agent(1), it may do so if it makes sure that the third party subscribes to the safe harbor principles or is subject to the Directive or another adequacy finding. As an alternative, the organization can enter into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant principles.

Access: Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

Security: Organizations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.

Data integrity: Personal information must be relevant for the purposes for which it is to be used. An organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.

Enforcement: In order to ensure compliance with these principles, there must be (a) readily available and affordable independent recourse mechanisms so that each individual's complaints and disputes can be investigated and resolved

and damages awarded where the applicable law or private sector initiatives so provide; (b) procedures for verifying that the commitments companies make to adhere to these principles have been implemented; and (c) obligations to remedy problems arising out of a failure to comply with the principles. Sanctions must be sufficiently rigorous to ensure compliance by the organization.

These principles may provide a useful point of departure for additional US law on data control and privacy protection. Following these principles would make it more difficult for foreign governments, terrorists or criminals to access sensitive and private information gathered by commercial activities for their own purposes. It would also limit commercial activities from obtaining and disclosing private data on US citizens for profit at the expense of citizen's interests.

It is a truism that excess regulation can stifle efficiency and innovation. Given the rapid pace of technological development and the importance of information technology to the US economy, this is a legitimate problem. However, it is also true that the lack of regulation of critical segments of society or the economy can have devastating effects, particularly where there is incentive for malfeasance. The very basic protections proposed here do not appear to have unduly impacted legitimate businesses when implemented as law in other nations.[56] Also, in the US, some corporations, including very large and profitable corporations like Ebay,[57] voluntarily abide by these principles and manage to compete and innovate quite successfully. While these protections cannot fully secure US citizen's private or sensitive data from a concentrated effort at collection,

56. EU has policy implementing these principles since 1998. Canada has had similar laws since 2004.

57. Ebay privacy policy available online at http://pages.ebay.in/help/policies/privacy-policy.html.

they can at least raise the cost and effort needed to do so, and with relatively little impact on legitimate commercial activity.

The political process and the Constitution should determine the balance of tradeoffs between data mining (for security purposes or otherwise) and privacy rights. Yet the IT-enhanced ability to collect and mine data and the current threat environment are such that either current US expectations for privacy or US laws and policy for protecting it will be forced to change. Achieving the desired outcome and fully executing The National Strategy for Information Sharing may not happen if policy does not react to, and make full use of, information technology's growing capability to augment and enhance surveillance and data mining.

Selected Bibliography

1. Bobitt, Philip. “The Warrantless Debate Over Wiretapping”. *New York Times*, August 22, 2007, A19.
2. Borland, John. “Maybe Surveillance is Bad After All”. http://www.wired.com/, (accessed August 08, 2007).
3. Burns, Robert. “Pentagon To Shut Down Controversial Anti-terror Database”. *Boston Globe*, August 22, 2007.
4. Cabena, Pablo. Pablo Hadjnian, Rolf Stadler, Jaap Verhees, Allesandro Zanasi. *Discovering Data Mining: From Concept to Implementation* (1997). Prentice Hall 1997.
5. Collins M., Timothy J. Shimeall, Sidney Faber, Jeff Janies, Rhiannon Weaver, Markus De Shon. *Predicting future botnet addresses with uncleanliness*. CERT Network Situational Awareness Group, Software Engineering Institute, May 9, 2007.
6. Densley J., Major, Lieutenant Jansen, Julie. *The Impact of Social Networking on the Vulnerability of US Air Force Personnel to Adversary Influence Operations,* Information Operations & Special Programs Division. Wright-Patterson AFB, Ohio 45433-7022, July 2007.
7. Economist Magazine, Unattributed. *Learning to live with Big Brother.* Economist Magazine, Sep 27th 2007.
8. Eggen, D. Key Part of Patriot Act Ruled Unconstitutional. Washington Post, September 30, 2004, A16.

9. Unattributed. *Federal judge rules 2 Patriot Act provisions unconstitutional.* CNN.com, http://www.cnn.com/2007/US/law/09/26/patriot.act/, (accessed September 26, 2007).
10. Granick, Jennifer. "Nation's Soul Is at Stake in NSA Surveillance Case". http://www.wired.com/, (Accessed August 15, 2007).
11. Grant, Greg. *Back to Iraq.* Government Executive, Posted online at www_GovernmentExecutive_com.htm. (accessed April 1, 2007).
12. Headquarters Department of the Army. FM 3-24, *Counterinsurgency.* (Washington, DC: Headquarters Department of the Army, December 2006).
13. Hosenball, Mark. "Dropped Call: The NSA's Threat Operations Center in Maryland". *Newsweek*, August 6, 2007.
14. Kalev, Sepp. *Best Practices in Counterinsurgency.* Military Review. May/June 2005, 8-12.
15. Kilcullen, David. *Counter Insurgency Redux.* Small Wars Journal, 2005. Posted online at http://www.smallwarsjournal.com/.
16. Landler, Mark and Markoff, John. "Digital Fears Emerge After Data Siege in Estonia". *New York Times*, May 29, 2007.
17. Leahy Patrick, Senate Judiciary Committee. *Hearing on "Privacy in the Digital Age: Discussion of Issues Surrounding the Internet*". April 21, 1999. Accessed online at http://judiciary.senate.gov/oldsite/42199pjl.htm.
18. Mendoza, Martha. "US Police Surveillance Questioned". *Associated Press*. Posted Online at http://www.cbsnews.com/, April 6, 2003.
19. Metz T., Lieutenant General, Colonel Tait, W., and Major McNealy, Michael. *OIF II, Intelligence Leads Successful Counterinsurgency Operations.* University

of Military Intelligence. http://www.universityofmilitaryintelligence.us (accessed 1 Sept, 2007).

20. Mitnick K., William Simon, Steve Wozniak. *The Art of Deception.* Wiley, October 4, 2002.
21. Nakashima, Ellen. "Terror Suspect List Yields Few Arrests". *Washington Post*, Page A01, Saturday, August 25, 2007.
22. Nordeste B., Carment, David. *A Framework for Understanding Terrorist Use of the Internet.* Canadian Centre for Intelligence and Security Studies, Norman Paterson School of International Affairs, Carleton University, 2006.
23. Palace, Bill. *Technology Note prepared for Management 274A Anderson Graduate School of Management at UCLA*. Spring 1996. Accessed online at http://www.anderson.ucla.edu/.
24. Poulsen, Kevin. "FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats". Online posting at http://www.wired.com/, August 18, 2007.
25. Schneier, Bill and Spitzner, Lance. *Know Your Enemy.* Pearson Education, August 2001.
26. Shane, Scott and David Johnston. "Mining of Data Prompted Fight Over US Spying". *New York Times*, July 29, 2007.
27. Shane, Scott and Lichtblau, Eric. "Cheney Pushed US to Widen Eavesdropping". *New York Times*, 14 May 2006.
28. Shimeall, Tim and Williams, Phil and Dunlevy, Casey. *Countering cyber war.* NATO Review, Winter 2001/2002.
29. Singel, Ryan. "Eavesdrop: How the FBI Wiretap Net Operates". http://www.wired.com/, (Accessed August 29, 2007)

30. Slobogin, Christopher. "Technologically – Assisted Physical Surveillance: The American Bar Association's Tentative Draft Standards" Harvard *Journal of Law & Technology.* Volume 10, Number 3 Summer 1997.
31. Sniffen, M. "DHS Ends Criticized Data-Mining Program". *Washington Post/Associated Press*, Sep 5, 2007.
32. Supreme Court of Errors of Connecticut. ^ *Griswold v. Connecticut*. 381 US 479.
33. Sweet, Jonathan E., Teamey, Kyle. *Organizing Intelligence for Counterinsurgency.* Military Review, 9/01/2006.
34. Tynan, Dan. "Astonishing! Spock Thinks You're a Pedophile". http://www.wired.com/, (accessed August 15, 2007).
35. US Air Force. Air Force Doctrine Document 2-3. *Irregular Warfare.* (Washington, DC: Department of the Air Force, August 2007).
36. US President. *December 17, 2003 Homeland Security Presidential Directive/HSPD-7.* (Washington DC: White House, December 17, 2003).
37. US President. *The National Strategy for Combating Terrorism.* (Washington DC: White House, September 2006).
38. US President. *National Strategy for Information Sharing.* (Washington DC: White House, October 2007).
39. US Senate Select Committee to Study Governmental Operations. *Intelligence Activities and the Rights of American,* (The Church Report). April 14, 1976.
40. US Congress. *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* (Public Law 107-56), also known as The Patriot Act. 107th Cong., 2001.

41. US Congress. *Protect America Act of 2007,* Public Law 110-55, S. 1927. 110th Cong., 2007.

42. US Congress. *The Foreign Intelligence Surveillance Act of 1978*, 50 U.S.C. §§1801-1811, 1821-29, 1841-46, and 1861-62. 95th Cong., 1978.

43. US Congress. *The Privacy Act of 1974,* 60 U.S.C. § 552a. 93rd Cong., 1974.

44. US Congress. *Electronic Communications Privacy Act of 1986*, 18 U.S.C. § 2510. 99th Cong., 1986.

45. US Congress. *Health Insurance Portability and Accountability Act of 1996(HIPAA).* Public Law 104-191, 105th Cong., 1996.

46. Vinge, Vernor. *True Names.* New York: Tom Doherty Associates, LLC, 2001.

47. Whittaker, Alan G., Smith C., McKune E. *The National Security Council and Interagency System.* Washington, D.C.: Industrial College of the Armed Forces, NDU, US DOD.